

AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listing, of claims in the application:

Listing of Claims:

1–35. (Canceled)

36–37. (Withdrawn)

38–39. (Canceled)

40. (Currently Amended) A method for constraining delegation of service requests made by a first server on behalf of a client, ~~by a client to a server, the method~~ comprising:

receiving, at the first server, an authentication mechanism for the client, wherein the authentication mechanism is generated using a first authentication method;

a server identifying, by the first server, a target service to which access is sought on behalf of [[a]] the client, wherein the target service is resident on a target server; ~~that has been authenticated using a first authentication method;~~

sending a request to a trusted third-party to issue a first service ticket to the first server for the client, wherein the first service ticket is adapted to be used with a second authentication method, and wherein the second authentication method is different from the first authentication method;

receiving, at the first server, the first service ticket to the first server, wherein the first service ticket to the first server specifies that the first service ticket is delegable through the presence of a forwardable flag in the first service ticket;

requesting, by the first server, a target service ticket from the trusted third-party configured for use by the first server to access the target service on behalf of the client, wherein the first server provides the trusted third-party with the first service ticket when requesting the target service ticket, and wherein the target service ticket is adapted to be used with the second authentication method; and

sending the target service ticket to the target server.

~~causing the server that is operatively coupled to the target service and the client to use a credential authenticating the server to request a service credential to itself from a second authentication method trusted third party by identifying the client and the first authentication protocol method; and~~

~~without participation of the client, causing the server to request from the second authentication method trusted third party a new service credential for use by the server and the target service, from the second authentication method trusted third party, wherein the server provides the trusted third party with the credential authenticating the server, information about the target service, and the service credential to itself.~~

41-42. (Canceled)

43. (Currently Amended) The method as recited in Claim 40, wherein the target service ticket service credential is configured for use by the server and the target service to which access is sought.

44-45. (Canceled)

46. (Currently Amended) The method as recited in Claim 40, wherein the first server is a front-end server, and wherein the target server is a back-end server that is coupled to the first server, with respect to a back-end server that is coupled to the front-end server, and wherein the back-end server is configured to provide the target service.

47. (Original) The method as recited in Claim 40, wherein the first authentication method is selected from a group of authentication methods comprising Passport, SSL, NTLM, and Digest.

48. (Original) The method as recited in Claim 40, wherein the second authentication method includes a Kerberos authentication protocol.

49. (Currently Amended) A computer-readable storage medium on a first server storing computer-executable instructions for performing tasks ~~for a method of~~

constraining delegation by a client to a server of service requests made by the first server on behalf of a client, the method comprising:

receiving, at the first server, an authentication mechanism for the client, wherein the authentication mechanism is generated using a first authentication method;

a server identifying, by the first server, a target service to which access is sought on behalf of a by the client, wherein the target service is resident on a target server; that has been authenticated using a first authentication method;

causing the server that is operatively coupled to the target service and the client to use a credential authenticating the server to request a service ticket to itself from a second authentication method trusted third party by identifying the client and the first authentication method protocol;

sending a request to a trusted third-party to issue a first service ticket to the first server for the client, wherein the first service ticket is adapted to be used with a second authentication method, and wherein the second authentication method is different from the first authentication method;

receiving, at the first server, the first service ticket to the first server, wherein the first service ticket to the first server specifies that the first service ticket is delegable through the presence of a forwardable flag in the first service ticket;

causing the server to requesting, by the first server, a [[new]] target service ticket from the trusted third-party configured for use by the first server to access the target service on behalf of the client, configured for use by the server to access the new service without participation of the client the identified service, from the second authentication method trusted third party, wherein the first server provides the trusted third-party with the first service ticket when requesting the target service ticket, and wherein the target service ticket is adapted to be used with the second authentication method; and credential authenticating the server to the client, information about the target service, and the service ticket to itself; and

sending the target service ticket to the target server.

causing the second authentication method trusted third party to issue the new service ticket allowing the server to directly access the new service when one of:

the service ticket specifies the service ticket is delegable; and

the second authentication method trusted third party maintains an indication that the service ticket is delegable.

50. (Currently Amended) The computer-readable medium as recited in Claim 49, wherein the ~~second authentication method~~ trusted third-party includes a key distribution center (KDC).

51. (Canceled).

52. (Currently Amended) The computer-readable medium as recited in Claim 49, wherein the ~~[[new]]~~ target service ticket is configured for use by the server and the target service.

53. (Currently Amended) The computer-readable medium as recited in Claim 49, further comprising authenticating the server to the trusted third-party, wherein ~~[[the]]~~ a credential authenticating the server to the trusted third-party includes a ticket granting ticket associated with the server.

54. (Canceled).

55. (Currently Amended) The computer-readable medium as recited in Claim 49, wherein the first server is a front-end server ~~with respect to a back-end server that is coupled to the front-end server~~, and wherein the target server is a [[the]] back-end server that is coupled to the front-end server ~~is configured to provide the target service~~.

56. (Original) The computer-readable medium as recited in Claim 49, wherein the first authentication method is selected from a group of authentication methods comprising Passport, SSL, NTLM, and Digest.

57. (Original) The computer-readable medium as recited in Claim 49, wherein the second authentication method includes a Kerberos authentication protocol.

58-61. (Canceled)

62. (New) A method, performed by a trusted third-party, of constraining delegation of service requests made by a first server on behalf of a client, the method comprising:

receiving, at the trusted-third party, a first request from the first server for a first service ticket, wherein the first server provides evidence that the client has been authenticated to the first server using a first authentication method, and wherein the first service ticket is a service ticket granting the client access to services on the first server;

sending the first service ticket to the first server, wherein the first service ticket is adapted to be used with a second authentication method, and wherein the second authentication method is different from the first authentication method;

receiving a second request from the first server to access a target server, wherein the first server is requesting to access the target server on behalf of the client, and wherein the second request comprises the first service ticket;

determining if the client has authorized delegation to the first server to request the access to the target service on the behalf of the client by checking the first service ticket for the presence of a forwardable flag; and

if the forwardable flag is present in the first service ticket, generating a target service ticket and sending the target service ticket to the first server;

if the forwardable flag is not present, denying the second request.

63. (New) The method of Claim 62, wherein the first authentication method is selected from a group of authentication methods comprising Passport, SSL, NTLM, and Digest.

64. (New) The method of claim 62, wherein the second authentication method includes a Kerberos authentication protocol.